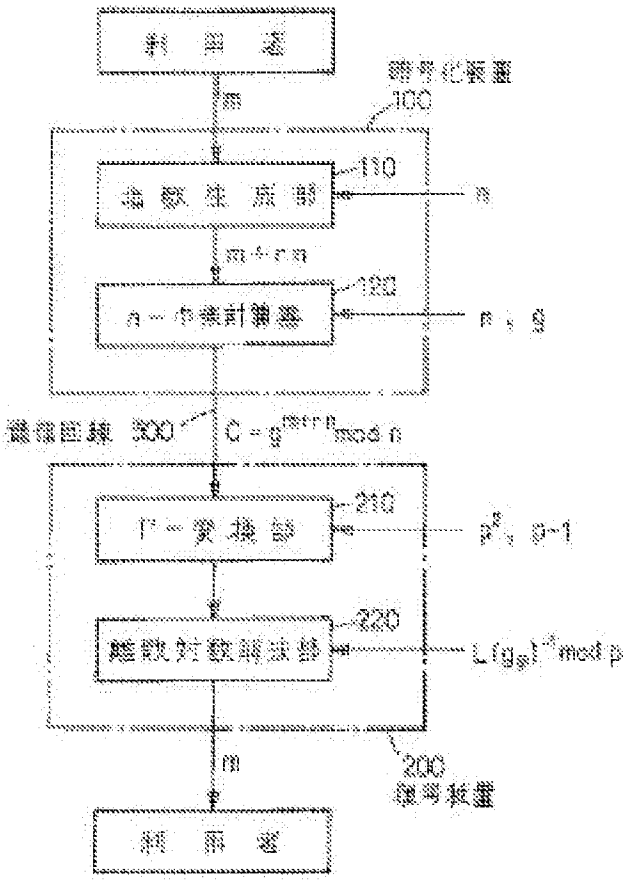
OPEN KEY CIPHERING DEVICE, OPEN KEY CIPHERING AND DECIPHERING DEVICE, AND DECIPHERING PROGRAM RECORDING MEDIUM

Publication number: JP11174955 (A)
Publication date: 1999-07-02
Inventor(s): UCHIYAMA SHIGENORI; OKAMOTO TATSUAKI
Applicant(s): NIPPON TELEGRAPH & TELEPHONE [JP]
Classification:
- international: ***G09C1/00;*** **G09C1/00;** (IPC1-7): G09C1/00
- European:
Application number: JP19970347613 19971217
Priority number(s): JP19970347613 19971217

Also published as:
JP3402441 (B2)

Abstract of **JP 11174955 (A)**

PROBLEM TO BE SOLVED: To guarantee safety, to efficiently solve a discrete logarithmic problem, and to make the processing quantity the same as before. SOLUTION: For add primes numbers (p) and (q), n=p<2> q and (g) are made open and (g) is selected out of (Z/nZ)* so that gp =g<r-1> mod p<2> has a location number (p) in (Z/p<2> Z)*; and m+rn is found (110) from a plaintext (m) and a random number (r) and C=g<m+rn> mod n is counted by using (n) and (g) to output a ciphertext (120). Then Cmodp<2> is found for C, (Cp -1)/p=L(Cp) is found, and a secret key L(gp) <-1> mod p is multiplied by L(Cp) to obtain a plaintext (m) (200).



Data supplied from the ***esp@cenet*** database — Worldwide

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号

特開平11－174955

(43)公開日　平成11年(1999)７月２日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０９Ｃ　1/00	６２０	Ｃ０９Ｃ　1/00	６２０Ａ
			６２０Ｚ

審査請求　有　　請求項の数14　ＯＬ　（全 13 頁）

(21)出願番号　特願平9－347613

(22)出願日　平成９年(1997)12月17日

(71)出願人　000004226
日本電信電話株式会社
東京都新宿区西新宿三丁目19番２号

(72)発明者　内山　成憲
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

(72)発明者　岡本　龍明
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

(74)代理人　弁理士　草野　卓

(54)【発明の名称】　公開鍵暗号化装置、公開鍵暗号復号装置及び復号プログラム記録媒体

(57)【要約】

【課題】　安全性を保証し、かつ離散対数問題を効率的に解き、処理量を従来と同様にする。

【解決手段】　奇素数ｐ，ｑに対し、ｎ＝ｐ^2 ｑと、ｇを公開し、ｇは（Ｚ／ｎＺ）* の中から、$g_p = g^{p-1} \bmod p^2$ が（Ｚ／ｐ^2 Ｚ）* の中で位数がｐとなるものから選定し、平文ｍと乱数ｒとｎからｍ＋ｒｎを求め（１１０）、ｎとｇを用い$C = g^{m+rn} \bmod n$を計数して暗号文を出力し（１２０）、Ｃに対し、$C \bmod p^2$ を求め、更に$C_p = C^{p-1} \bmod p^2$ を計算し（２１０）、$(C_p - 1)/p = L(C_p)$ を求め、秘密鍵Ｌ$(g_p)^{-1} \bmod p$をＬ（C_p）に乗算して平文ｍを得る（２００）。

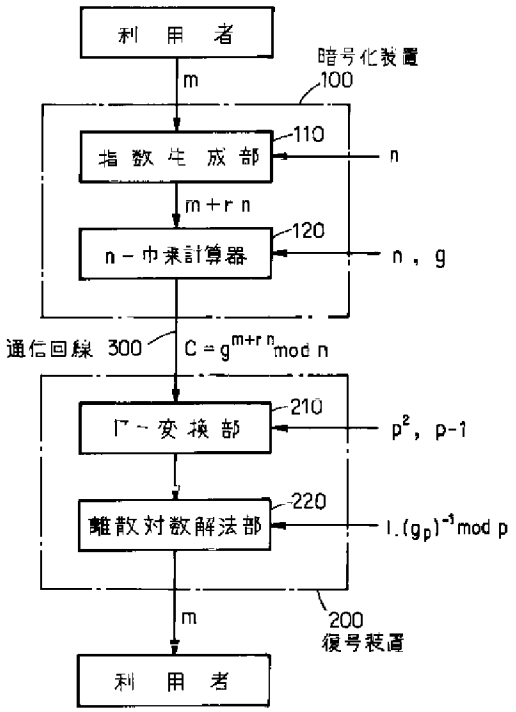


図１

【特許請求の範囲】

【請求項１】　入力された平文と乱数を組み合わせて指数を生成する指数生成手段と、
合成数よりなる第１公開鍵を法とした既約剰余類群において第２公開鍵を上記指数で巾乗計算して暗号文を出力する巾乗計算手段とを具備する公開鍵暗号化装置。

【請求項２】　ｐ，ｑを同一ビット数の奇素数とすると、上記第１公開鍵はｎ＝ｐ^2 ｑであり、上記第２公開鍵ｇは、ｎを法とする既約剰余類群（Ｚ／ｎＺ）* の中から、$g_p = g^{p-1} \bmod p^2$ が（Ｚ／ｐ^2 Ｚ）* の中での位数がｐとなるものから選定されていることを特徴とする請求項１記載の公開鍵暗号装置。

【請求項３】　入力された暗号文を、合成数よりなる第１公開鍵を法とし既約剰余類群の元C_p に、第１秘密鍵を用いて変換するΓ－変換手段と、
上記変換された元C_p における離散対数と第２秘密鍵を用いて解いて復号平文を得る離散対数解法手段と、を具備する公開鍵暗号復号装置。

【請求項４】　ｐ，ｑを奇素数、ｎ＝ｐ^2 ｑ、上記入力暗号文Ｃを０＜Ｃ＜ｎの範囲にある整数で、ｎと互いに素であるものとし、上記ｐを上記第１秘密鍵とし、上記ｎを上記第１公開鍵とし、
上記Γ－変換手段は、$C \bmod p^2 \in (Z / p^2 Z)^*$ を計算する ｐ^2 －還元手段と、
その ｐ^2 －還元手段の計算結果$C \bmod p^2$ に対し ｐ^2 を法とするｐ－１の巾乗計算を行って上記元C_p を得る変換手段とよりなることを特徴とする請求項３記載の公開鍵暗号復号装置。

【請求項５】　上記第１秘密鍵ｐを奇素数としg_p 、上記C_p を$0 < g_p , C_p < p^2$ の範囲にある整数で、$g_p \equiv C_p \equiv 1 \pmod 1$、$g_p \neq 1 \pmod{p^{-2}}$ を満し、$((g_p - 1) / p)^{-1} \bmod p$ を上記第２秘密鍵とし、
上記離散対数解法手段は、上記元C_p を入力してＬ（C_p ）＝（C_p －１）／ｐを演算する対数計算手段と、
その演算結果Ｌ（C_p ）と上記第２秘密鍵との積を上記ｐを法として求めて復号平文を出力する乗算手段とよりなることを特徴とする請求項３又は４記載の公開鍵暗号復号装置。

【請求項６】　公開鍵ｎ，ｇを用いる暗号化装置の暗号化処理を実行するプログラムを記録した記録媒体において、
上記プログラムは、
乱数ｒを生成する過程と、
上記乱数ｒと上記公開鍵ｎを乗算する過程と、
その乗算結果ｒｎと入力平文ｍを加算する過程と、
上記公開鍵ｎを法として、上記公開鍵ｇに対し上記加算値ｎ＋ｒｎを巾乗計算して暗号文Ｃを出力する過程とよりなることを特徴とするコンピュータ読出し可能な記録媒体。

【請求項７】　ｐ，ｑを同一ビット数の奇素数とすると、上記公開鍵ｎはｐ^2 ｑであり、上記公開鍵ｇは、ｎを法とする既約剰余類群（Ｚ／ｎＺ）* の中から、$g_p = g^{p-1} \bmod p^2$ が（Ｚ／ｐ^2 Ｚ）* の中での位数がｐとなるものから選定されていることを特徴とする請求項６記載の記録媒体。

【請求項８】　ｐ，ｑを奇素数、ｎ＝ｐ^2 ｑを公開鍵とし、入力暗号文Ｃを０＜Ｃ＜ｎの範囲にある整数で、ｎと互いに素であるものとし、入力暗号文Ｃを復号する復号装置の処理を実行するプログラムを記録した記録媒体であって、
上記プログラムは、
上記入力暗号文Ｃに対し、ｐ^2 を法とする既約剰余類群の元$C \bmod p^2$ を求める過程と、
上記$C \bmod p^2$ に対し、ｐ^2 を法とするｐ－１の巾乗演算を行って元C_p を求める過程と、
上記元C_p における離散対数を秘密鍵を用いて解いて復号平文を出力する離散対数解法過程と、
を有することを特徴とするコンピュータ読出し可能な記録媒体。

【請求項９】　g_p 、上記C_p を$0 < g_p , C_p < p^2$ の範囲にある整数で$g_p \equiv C_p \equiv 1 \pmod q$、$g_p \neq 1 \pmod{p^2}$ を満し、上記秘密鍵は$((g_p - 1) / p)^{-1} \bmod p$であり、
上記離散対数解法過程は、
上記元C_p と上記ｐとを用い（C_p －１）／ｐを計算する過程と、
ｐを法として上記（C_p －１）／ｐに上記秘密鍵を乗算して上記復号平文を得る過程とよりなることを特徴とする請求項８記載の記録媒体。

【請求項１０】　入力された平文と乱数を組み合わせて指数を生成する指数生成手段と、
合成数よりなる第１公開鍵を法として剰余類環上との楕円曲線における巾乗計算と、上記指数を指数とし、第２公開鍵に対して行って暗号文を出力する巾乗計算手段と、
を具備する公開鍵暗号化装置。

【請求項１１】　入力された暗号文を有限素体上の楕円曲線を元C_p に変換する還元手段と、
上記元C_p に対する、離散計数を求めて、復号平文を出力するＳＳＡアルゴリズム手段と、
を具備する公開暗号復号装置。

【請求項１２】　ｐを奇素数（＞５）、E_p を有限体F_p 上の楕円曲線でそのF_p 有理点の個数がｐとなるものとし、このF_p －有理点をG_p ，C_p （どちらも無限遠点でない）とし、$\lambda(G_p)^{-1} \bmod p$ を秘密鍵とし、
上記ＳＳＡアルゴリズム手段は、
上記元C_p と上記ｐ、上記楕円曲線E_p 、上記関数λを入力してλ（C_p ）を計算する対数計算手段と、
上記λ（C_p ）と、上記秘密鍵を入力して、両者の積を

上記ｐを法として求めて上記復号平文を出力する乗算手段とよりなることを特徴とする請求項１１記載の公開鍵暗号復号装置。

【請求項１３】　公開鍵ｎ，Ｇ，F_p 有理点の個数がｐの有限体F_p 上の楕円曲線E_p ，F_q 有理点の個数がｑの有限体F_q 上の楕円曲線E_q から中国人剰余定理を用いて得られるｎを法とした剰余類環上の楕円曲線を用いる暗号化装置の暗号化処理を実行するプログラムを記録した記録媒体において、

上記プログラムは、

乱数ｒを生成する過程と、

上記乱数ｒと上記公開鍵ｎを乗算する過程と、

その乗算結果ｒｎと入力平文ｍを加算する過程と、

合成数よりなる第１公開鍵を法として剰余環上の楕円曲線における巾乗計算を、上記加算値を指数とし第２公開鍵に対して行って暗号文を出力する巾乗計算過程と、

を有するコンピュータ読出し可能な記録媒体。

【請求項１４】　ｐを奇素数（＞５）、E_p を有限体F_p 上の楕円曲線でそのF_p －有理点の個数がｐとなるものとし、この二つのF_p 有理点G_p ，C_p （どちらも無限遠点でない）とし、$\lambda(G_p)^{-1} \bmod p$ を秘密鍵とし、入力暗号文Ｃを復号する復号装置の処理を実行するプログラムを記録した記録媒体であって、

上記プログラムは、

上記入力された暗号文Ｃを有限素体上の上記楕円曲線の元C_p に、上記ｐを法として変換する過程と、

上記元C_p に対し、Ｅ（F_p ）からF_p への写像関数λを演算してλ（C_p ）を求める過程と、

上記λ（C_p ）と上記秘密鍵の積を、上記ｐを法として求めて復号平文を出力する過程と、

を有するコンピュータ読出し可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は公開鍵暗号方式に用いる暗号装置、復号装置、その処理プログラムを記録した記録媒体に関する。

【０００２】

【従来の技術】機密保持性のない通信回線を介してデータを送受信する場合、送受信のデータの盗聴防止に暗号法が用いられる。一般に、暗号法は共通鍵暗号と公開鍵暗号の二種類に区別できる。共通鍵暗号は暗号鍵と復号鍵が同じなので、鍵を秘密に配送する必要がある。また、通信の組合せ数と同じ数だけ鍵を必要とするので、ネットワーク内の送受信局数が増加すると、秘密に管理する鍵の数が急激に増加することが問題となる。

【０００３】一方、公開鍵暗号は、暗号鍵と復号鍵が異なっており、暗号鍵を公開しても、暗号鍵から復号鍵を算出することが計算量的に難しければ、秘密鍵の秘密性は損なわれないので、暗号鍵の配送が不用である。また、各送受信局は自分の復号鍵だけを秘密に管理するので、秘密に管理する鍵の問題も解決できる。即ち、公開鍵暗号を利用すれば、共通鍵暗号を利用する時に問題であった鍵の管理の問題が解決される。また、共通鍵暗号を使う時の一番大きな問題であった、鍵配送の問題が解決出来る、即ち、鍵を秘密に配送する必要がない。また、共通鍵暗号では、鍵が当時者間で共有されているため、共通の鍵で作成された暗号文は、同鍵を所有する二人のうちいずれかが作成したかが特定することが出来ない。一方、公開鍵暗号では、秘密鍵を有するものが唯一であるため、同鍵で暗号化された文章を作成出来るのは、同鍵を持つもの唯一であるという意味で、証拠性を持ち得る。この性質を、ディジタル署名と言う。

【０００４】即ち、公開鍵暗号を用いれば、ディジタル署名が実現出来、通信の相手を認証することに利用出来る。公開鍵暗号は、一方向性落し戸関数と呼ばれるものを使えば実現できることが知られている。一方向性関数とは、一方から他方への計算は簡単であるが、その逆を計算することは、計算量的に難しい関数のことで、その一方向性関数に「ある秘密を知っていれば、逆も簡単に計算できる」というしかけをもたせたものを一方向性落し戸関数と言い、そのしかけを「落し戸」と呼ぶ。現在のところ、素因数分解問題（合成数を入力とし、その合成数の素因子を出力する関数と、素因数分解することは同一視することが出来る。以下、ＩＦＰと表す。以下にあげる問題も、これと同様にある関数と同一視することが出来る）、有限体の乗法群における離散対数問題（例えば、ｐを素数として、有限素体F_p の乗法群$F_p^* = <g>$において、その乗法群の元ｙが与えられているとき、$y = g^x$ なる、整数ｘで$0 \leq x < p$を満たすものを求める問題、以下、ＤＬＰと表す。）、有限体上の楕円曲線における離散対数問題（例えば、ｐを素数として、有限素体F_p 上定義された楕円曲線ＥのF_p －有理点全体のなす群Ｅ（F_p）、その一つの点Ｇ、点Ｇで生成されるＥ（F_p ）の部分群の点Ｐが与えられている時、Ｐ＝ｍＧを満たす整数ｍを求める問題、以下、ＥＣＤＬＰと表す、但し、ｍＧは、楕円曲線上の加法でＧをｍ倍した点を表す。楕円曲線、及び楕円曲線暗号に関しては、例えば、Menezes , A.J.著“Elliptic Curve Public Key Cryptosystems ”, Kluwer Academic Publishers（1993）を参照。以下、この文献を文献１と称す）などが、一方向性関数であろうと予想されているものの代表的なものであり、現在提案されている公開鍵暗号の中で、代表的かつ実用的なものは、ＲＳＡ暗号、Rabin 暗号、ElGamal 暗号、楕円曲線暗号（楕円ElGamal 暗号）が挙げられると思われるが、ＲＳＡ暗号、Rabin 暗号はＩＦＰの難しさ、ElGamal 暗号は、ＤＬＰの難しさ、楕円曲線暗号は、有限体上の楕円曲線の点のなす群におけるElGamal 暗号で、これはＥＣＤＬＰの難しさに、それぞれ基づくものである。

【０００５】ＲＳＡ暗号については、Communication of

the ACM, vol.21, pp.120-126(1978)に、Rivest, R.L.等によって、“A Method for Obtaining Digital Signatures and Public-Key Cryptosystems”と題して論及されており（以下、この文献を文献２と称す）、Rabin 暗号については、MIT , Technical Report, MIT/LSC/TR-212(1979)にRabin , M.O.によって、“Digital Signatures and Public-Key Functions as intractable as Factorization ”と題して論及されている（以下、この文献を文献３と称す）、さらに、ElGamal 暗号についてはＩＥＥＥ Trans.on Information Theory, 1T-31 , ４, pp.469-472(1985)に、ElGamal Ｔ. によって、“A Public-Key Cryptosystem and a Signature Scheme Based on DiscreteLogarithms ”と題して論及されており（以下、この文献を文献４と称す）、楕円曲線暗号については、Miller, Ｖ. Ｓ. とKoblitz , Ｎ. によって、１９８５年に独立に提案されたものであるが、Proc.of Crypto'85 , LCNCS 218 , Springer-Verlag , pp.417-426(1985)にMiller, Ｖ. Ｓ. によって“Use of EllipticCurves in Cryptography”と題して論及され（以下、この文献を文献５と称す）、Math.Comp., 48, 177 , pp.203-209(1987)にはKoblitz , Ｎ. によって“Elliptic Curve Cryptosystems”と題して論及されている（以下、この文献を文献６と称す）。

【０００６】以下、具体的にこれらの暗号を紹介をし、その性質について述べる。ＲＳＡ暗号の構成法は次の通りである。異なる奇素数ｐ，ｑを選び、ｎ，ｅ，ｄを次の式を満たすように取る。

$$n=pq,$$

$$GCD(e, LCM(p-1, q-1))=1,$$

$$ed\equiv 1 \pmod{LCM(p-1, q-1)}$$

ここで、ＧＣＤ（ａ，ｂ）は、整数ａ，ｂの最大公約数，ＬＣＭ（ａ，ｂ）は、整数ａ，ｂの最小公倍数を表すものとする。

【０００７】（ｎ，ｅ）を公開鍵（ｄ，ｐ，ｑ）を秘密鍵として、暗号化処理（E_1 ）と復号処理（D_1 ）を

$$C\equiv E_1(M)\equiv M^e \pmod{n} \quad (1)$$

$$M\equiv D_1(C)\equiv C^d \pmod{n} \quad (2)$$

で定義する。この時、Mが$0<M<n-1$を満たすなら

$$D_1(E_1(M))=M \quad (3)$$

が成り立つ。

【０００８】Rabin 暗号の構成法は次の通りである。ｐ，ｑ，ｎを上述の通りに取り、さらに、$0<b<n$を

$$C\equiv E_2(M)\equiv M(M+b) \pmod{n} \quad (4)$$

$$M\equiv D_2(C)\equiv (-b\pm\sqrt{(b^2+4C)})/2 \pmod{p\text{かつ}\bmod q} \quad (5)$$

で定義する。Rabin 暗号は、復号時に連立方程式を解くことになるが、二次方程式は二つの解を持つので、一般には四つの解が現れてきて、上のままでは復号が一意に出来ないという問題があった。これは、なんらかの付加的な情報を付けて通信を行なう、即ち、運用上の問題として回避することも出来るし、一意に復号出来るように改良もされている。これに関しては、電子情報通信学会論文誌、Vol.J70-A , No. １１, pp.1632-1636(1987)に、黒澤　馨等によって“素因数分解の困難さと同等の強さを有する逆数を利用した公開鍵暗号”と題して論及されている。（以下、この文献を文献７と称する）

また、ElGamal 暗号の構成は次の通りである。ｐを素数、ｇを、ｐを法とした既約剰余類群$(Z/pZ)^*$の一つの生成元、即ち、位数がｐ－１の元とし、$0<x<p$なる整数ｘを任意に取り、$y\equiv g^x \pmod{p}$とおく。この時、（ｙ，ｇ，ｐ）を公開鍵、ｘを秘密鍵として、暗号化処理（E_3 ）、復号処理（D_3 ）を

$$C=(C_1, C_2)=E_3(M) \quad (6)$$

$$C_1\equiv g^r \pmod{p} \quad (7)$$

$$C_2\equiv y^r M \pmod{p} \quad (8)$$

$$M\equiv D_3(C)\equiv C_2/C_p{}^x \bmod p \quad (9)$$

で定義する。ここで、ｒは、$0<r<p$なる任意の整数とし、暗号化処理をするたびに選ぶものとする。

【０００９】Mが$0<M<p$であれば、

$$M=D_3(E_3(M)) \quad (10)$$

が成立する。楕円曲線暗号（楕円 ElGamal暗号）の構成は次の通りである。ｐを素数、有限素体F_p 上の楕円曲線$E(a, b): y^2=x^3+ax+b \ (a, b\in F_p, 4a^3+27b^2\neq 0)$、楕円曲線上の$F_p$ －有理点Ｇで、その位数ｑが十分大きな素数を約数に持つものとする。$0<x<q$なる任意の整数を取り、$E(a, b)$上の加法で$P=xG$とする。この時、（ｐ，Ｅ（ａ，ｂ），Ｇ，Ｐ，ｑ）を公開鍵、ｘは秘密鍵として暗号化処理（E_4 ）、復号処理（D_4 ）を

$$C=(C_1, C_2)=E_4(M) \quad (11)$$

$$C_1=rG_1 \quad (12)$$

$$C_2 = rP + M \quad (13)$$

$$M = D_4\ (C) = (C_2 - xC_1\ \text{のX－座標}) \quad (14)$$

で定める。ここで、ｒは０＜ｒ＜ｑを満たす任意の整数とし、暗号化処理のたびに選ぶものとする。また、ｒＰ＋Ｍは、Ｘ－座標がＭとなる楕円曲線上の点と点ｒＰとの楕円曲線上での和を表すものとする。一般には、常にＭをＸ－座標に持つ点が、与えられた楕円曲線上に存在するかどうかは分からないが（ここでの場合は、確率１／２で点が存在する）、何らかの、システムに共通の規則を定めてＭにある程度の冗長情報を付加することによって、常に、冗長情報を付加したものをＸ－座標に持つような点が取れるように出来る。

【００１０】次に、上述の暗号の計算量について述べる。ＲＳＡ暗号の計算量は、暗号化処理、復号処理が共にk^3 のオーダーで実現されることが知られている。ここで、ｋは公開鍵ｎのビット数を表すとする。Rabin 暗号の計算量は、暗号化処理はk^2 のオーダーで、復号処理はk^3 のオーダーで実現される。このｋも公開鍵ｎのビット数を表すものとする。

【００１１】ElGamal 暗号の計算量は、暗号化処理、復号処理共にk^3 のオーダーで実現できる。ここで、ｋは、公開鍵である素数ｐのビット数を表すものとする。さらに、楕円曲線暗号の計算量は、暗号化処理、復号処理共にk^3 のオーダーで実現できることが知られている。ここで、ｋは公開鍵である素数ｐのビット数であるとする。

【００１２】オーダーで比較するなら、上述の暗号は計算量はあまり変わらないが、実装させると、差が出てくることは明らかである。実際、楕円曲線上の加法は、その定義体である有限体における乗法の１０倍程度時間がかかることが知られている。次に、安全性について述べる。暗号は、攻撃者（盗聴者）に通信内容を隠して送ることを目的とするため、どの程度通信内容を隠しているかの度合が重要になる。即ち、秘匿性としては、完全解読（暗号文から、平文が完全に求められる事）と部分解読（暗号文から、平文の部分情報が求められる事）の二種類に分類できる。次に、公開鍵暗号の攻撃者のタイプには、単に暗号通信を受信し、その情報だけから解読を試みる受動的攻撃と、送信者に様々な質問とし（暗号文を送り）、その回答（その復号結果）をもらうことが許され、それらの情報をもとにして、目的とする暗号文を解読するような能動的攻撃の二種類に分けられる。特に、能動的攻撃の中でも、適応的選択暗号文攻撃（解読者が任意に選んだ暗号文を真の受信者に復号させた後、そこで得た情報と公開情報を用いて、別の暗号文を復号する攻撃）がもっとも強力である。

【００１３】さて、そこで、これらの分類を元に、上述の代表的な公開鍵暗号の安全性について述べることにすると、ＲＳＡ暗号、Rabin 暗号のようなＩＦＰの難しさに基づく暗号は、公開鍵ｎを素因数分解出来れば、秘密鍵である素数ｐ，ｑが分かり、ＬＣＭ（ｐ－１，ｑ－１）が計算出来て、秘密鍵ｄが求められ、安全に解読されてしまう、ここで、ＬＣＭ（ｐ－１，ｑ－１）を、ｎだけから求めようとすることは、ｎを素因数分解することと等価であることが証明されている。即ち、ｐ，ｑが分からないままで、ＬＣＭ（ｐ－１，ｑ－１）を求めることは出来ない。しかし、ＲＳＡ暗号は、公開鍵ｎを素因数分解する以外の方法で完全解読出来る可能性が残っているが、Rabin 暗号を完全解読する方法は、公開鍵ｎを素因数分解する以外にないことが証明されている。即ち、ＲＳＡ暗号を解読することはＩＦＰを解くことと等価であるかどうかは未解決であるが、Rabin 暗号の完全解読は、ＩＦＰを解くことと等価であることが証明されている。（上述の逆数暗号も、ＩＦＰと等価であることが証明されている）このRabin の結果は、ある基本的な問題（今の場合、ＩＦＰ）が難しいであろうと仮定することによって、暗号のある種の安全性が証明出来ることを初めて示したものである。今の場合、上述の公開鍵暗号の安全性で言えば、受動的攻撃に対して安全であることが、ＩＦＰの難しさを仮定した上で、証明されたことを意味している。部分解読に関しては、ＲＳＡ暗号、Rabin 暗号共に、暗号文Ｃから、平文Ｍの最下位ビットを求めることは、Ｃから、Ｍ全体を求めることと同じ位難しいことが証明されている。また、さらに同様にＭの最下位よりlog ｋ ビットの部分が同様の安全性を持つことが証明されている。この事実は、SIAM Journal of Computing , 17, ２, pp.449-457(1988)において、Alexi , W. 等によって、“ＲＳＡ and Rabin Functions：Certain Patrs Are as Hard as the Whole”と題して論及されている。（以下、この文献を文献８と称す）

次に、ElGamal 暗号の安全性についてであるが、これはＤＬＰの難しさに基づく暗号であるので、ＤＬＰが解ければ、公開鍵（ｙ，ｇ，ｐ）から、秘密鍵ｘが求められ、解読されてしまう。しかし、ElGamal 暗号の解読がＤＬＰと同じ程度に難しいかどうかは証明されていない。同様に、楕円曲線暗号についても、ＥＣＤＬＰと同じ程度に難しいかどうかは証明されていない。

【００１４】以上、代表的かつ実用的な公開鍵暗号について説明したが、基本的な問題の難しさを仮定し、ある種の安全性が証明出来る公開鍵暗号は、Rabin 暗号とその変形位しか知られていない。つまり、実用性を考えると、一方向性関数としてつかえるものは、ＩＦＰ，ＤＬＰとＥＣＤＬＰ位しか知られてなく、これらを使って新しい「落し戸」を作り、それを用いてある種の安全性の証明のついた新しい公開鍵暗号システムを作ることは一つの問題である。

【００１５】

【発明が解決しようとする課題】上述のように、公開鍵

暗号は、従来からの共通鍵暗号と比較すれば、鍵管理の問題を解決することが出来、ディジタル署名を実現することが出来るが、実用的な公開鍵暗号を実現するには、一方向性関数としてはＩＦＰ，ＤＬＰやＥＣＤＬＰ位しか知られてなく、これらを用いて「落し戸」を作る作り方も本質的にこれ等位しか知られてなく、ましてや、ある種の安全性が証明されている暗号は、Rabin 暗号とその変形だけである。

【００１６】この発明の目的は、一方向性関数としてはＩＦＰを用いながらも、新しい「落し戸」を用いて、ＩＦＰが難しいであろうという仮定に基づき、受動的攻撃に対して安全であることが証明できる公開鍵暗号装置を提供することである。

【００１７】

【課題を解決するための手段】具体的には、この発明は二種類の公開鍵暗号装置を提供する。ｐ，ｑを二つの素数として、$n=p^2q$としたとき、ｎを法とした既約剰余類群（Ｚ／ｎＺ）*上で構成されるものと、$n=pq$としたとき、ｎを法とした剰余類環Ｚ／ｎＺ上で定義される楕円曲線E_n 上で構成される公開鍵暗号装置との二つを提供する。以下、前者を「乗法群に基づく公開鍵暗号装置」と呼び、後者を「楕円曲線に基づく公開鍵暗号装置」と呼ぶことにする。

【００１８】有限素体F_p 上の楕円曲線で、位数がｐのものを anomalous楕円曲線と呼ぶことにする。この anomalous楕円曲線上の離散対数問題が非常に効率良く計算出来ることが、Smart,N.P.によって、“ The Discrete Logarithm Problem on Elliptic Curves of Trace one, preprint(September,1997)”において（以下、この文献を文献９と称す）、佐藤考和等によって、“Fermat Quotient and the Polynomial Time Discrete Logarithm for Anomalous Elliptic Curves,preprint(September,1997) ”において（以下、この文献を文献１０と称す）、それぞれ独立に論及されている。この anomalous楕円曲線における離散対数問題を解くアルゴリズムを、以下ではＳＳＡアルゴリズムと呼ぶことにする。

【００１９】特に、後者の論文中で示唆されていることとして、ある種の群のp-Sylow 部分群における離散対数問題が、非常に効率良く解けるという事実がある。ここで、p-Sylow 部分群とは、例えば、有限群Ｈが与えられているとき、Ｈの部分群の中で、位数がｐの幅となるものの中で最も位数が大きなものをＨのp-Sylow 部分群という。この発明では、このある種の群のp-Sylow 部分群における離散対数問題が非常に効率良く解けることを利用して、ある種の安全性の証明がつけられる、新しい公開鍵暗号を提供する。

【００２０】ｐを奇素数として、p^2 を法とした既約剰余類群（Z/p^2Z）* において、そのp-Sylow 部分群Γ、即ち、この場合は位数ｐの部分群になるが、これは次のように書ける：

$$\Gamma=\{x\in(Z/p^2Z)^* \mid x\equiv 1 \pmod p\} \tag{15}$$

（Z/p^2Z）* における離散対数問題は、現在のところ、非常に難しい問題であると信じられていて、効率の良いアルゴリズムはまだ発見されていない、しかし、Γにおける離散対数問題は非常に効率良く解ける。実際、次のようなΓ上定義された関数を考える：

$$L(x)=(x-1)/p,\ x\in\Gamma \tag{16}$$

この関数の値は、有限素体F_p にとるとみなせる。すると、この関数Ｌは、任意のａ，ｂ∈Γに対して

$$L(ab)=L(a)+L(b) \bmod p \tag{17}$$

なる性質を持つことが簡単に分かり、この関数は、ΓからF_p への群としての同型写像を与えていることも分かる。このＬの計算量は、ｐのビット数をｋとすればk^2 のオーダーであることが簡単に分かる。従って、Γにおける離散対数問題、即ち、ｘ∈Γ，ｍを０＜ｍ＜ｐから任意とり、$y=x^m$ とおいて、ｘ，ｙからｍを求める問題については、式（17）から

$$L(y)=L(x^m)=mL(x) \bmod p \tag{18}$$

となるので、$L(x)\neq 0 \bmod p$であれば

$$m=L(y)/L(x) \bmod p \tag{19}$$

と、効率良く求めることが出来る。ｘ，ｙから、ｍを求める計算量は、ｐのビット数をｋとすれば、k^3 のオーダーで出来る。

【００２１】この性質を用いれば、全く新しい「落し戸」が構成出来、新しい公開鍵暗号が構成出来る。まず、中国人剰余定理（中国人剰余定理は、例えば、岡本・山本著、“現代暗号”、ｐｐ．１５、産業図書（１９９７）を参照。以下、この文献を文献１１と称す）より

$$(Z/nZ)^* \sim (Z/p^2Z)^* \times (Z/qZ)^* \tag{20}$$

$$\sim \Gamma\times(Z/pZ)^* \times (Z/qZ)^* \tag{21}$$

が成り立つので、「乗法群に基づく公開鍵暗号装置」は、以下で定められる：$g\in(Z/nZ)^*$ で$g_p=g^{p-1} \bmod p^2\in\Gamma$が$L(g_p)\neq 0 \bmod p$を満たすものを取り、ｎ，ｇ，ｋを公開鍵とする。ここで、ｋは、素数ｐ，ｑのビット数とする。平文ｍを$0<m<2^{k-1}$ から取る自然数とすると、ｒをＺ／ｎＺから任意に取り、暗号化を次で定める

$$C=g^{m+rn} \bmod n \tag{22}$$

復号は、ＣをΓの元に変換することが出来れば、ｎの素因子ｐを知っているものは、上述の関数Ｌを用いて効率良くその離散対数を求めることが出来、ｍは０＜ｍ＜２

$$C_p = C^{p-1} \bmod p^2$$

とすれば、$C_p \in \Gamma$となり、上記Ｌ関数を用いて離散対数を効率的に解くことができる。また、この公開鍵暗号を解読することは、公開鍵ｎを素因数分解することと、即ち、ＩＦＰと等価であることが証明できる。

【００２２】この発明の「乗法群に基づく公開鍵暗号装置」においては、暗号化装置は、平文と乱数を組み合わせて、法ｎで巾乗計算のための指数部分を生成する指数生成部、mod ｎでの巾乗計算を行う、ｎ－巾乗計算器からなり、ｎ－巾乗計算器で生成された暗号文を通信回線

$$E_p : y^2 = x^3 + a_p x + b_p \quad (a_p, b_p \in F_p, 4a_p^3 + 27b_p^2 \neq 0), \quad (24)$$

$$E_q : y^2 = x^3 + a_q x + b_q \quad (a_q, b_q \in F_q, 4a_q^3 + 27b_q^2 \neq 0), \quad (25)$$

$a = a_p \bmod p$、$b = b_p \bmod p$、$a = a_q \bmod q$、$b = b_q \bmod q$なるａ、ｂは、中国人剰余定理よりmod ｎ

$$E_n : y^2 = x^3 + ax + b \ (a, b \in Z/nZ, GCD(4a^3 + 27b^2, n) = 1) \quad (26)$$

を得る。以下、特別にことわらない限りは、上述のように中国人剰余定理を用いて得られる関係にあるものは

$$E_n = [E_p, E_q], \ a = [a_p, a_q], \ b = [b_p, b_q] \quad (27)$$

などと表すことにする。また、特に、法を強調したいときは

$$E_n = [E_p \bmod p, E_q \bmod q] \quad (28)$$

などともあらわすことにする。

【００２４】今、E_p は anomalous楕円曲線、E_q は anomalousでない楕円曲線とする。このとき、上述の「乗法群に基づく公開鍵暗号装置」と同様にｎ、E_n、E_n（Ｚ／ｎＺ）の点Ｇ，ｋを公開鍵としておく。但し、Ｇは十分大きな（例えばビット数がｎと同じ）位数を持つものとしておき、ｋは、素数ｐ、ｑのビット数とする。このとき、平文ｍを$0 < m < 2^{k-1}$ から取ることにすると、ｒをＺ／ｎＺから任意に取り、暗号化を次で定める

$$C = (m + rn)G \in E_n \ (Z/nZ) \quad (29)$$

復号は、ｎの素因子ｐを知っているものは、この暗号文の定義式をmod ｐとして、E_p（F_p）の点の間の関係式に変換することが出来るので、上述のＳＳＡアルゴリズムを用いて効率良くその離散対数を求めることが出来、したがって効率良く復号が出来る。また、この公開鍵暗号を解読することは、公開鍵ｎと anomalous楕円曲線と anomalousでない楕円曲線から中国人剰余定理を用いて得られるＺ／ｎＺ上の楕円曲線E_n，点Ｇが与えられたとき、これから、ｎを素因数分解することと等価であることが証明できる。即ち、このｎ、E_nと、その曲線上の点Ｇが与えられたとき、ｎを素因数分解する問題を、変形素因数分解問題（以下では、ＭＩＦＰと表すことにする）と呼ぶことにすると、この楕円曲線E_nを用いた暗号を解読することは、ＭＩＦＰと等価であることが証明できる。

【００２５】この発明の「楕円曲線に基づく公開鍵暗号装置」においては、暗号化装置は、平文と乱数を組み合わせて、E_n（Ｚ／ｎＺ）における幅乗計算のための指数部分を生成する指数生成部、E_n（Ｚ／ｎＺ）での幅$k-1$ の範囲にあるので、mod ｐでは一意に定まり、したがって、効率良く復号が出来る。Ｃを Γの元に変換する方法は、

に送出する。一方、復号装置は、法p^2 でのｐ－１乗計算を行う、Γ－変換部とΓにおける離散対数問題を解いて復号する、離散対数解法部からなる。

【００２３】次に、この発明の「楕円曲線に基づく公開鍵暗号装置」について述べる。これに対しても同様に、二つの素数ｐ，ｑを取り、ｎ＝ｐｑとし、F_p、F_q 上の楕円曲線E_p、E_q がそれぞれ次で与えられているとする：

【００２６】

【発明の実施の形態】はじめに、この発明による「乗法群に基づく公開鍵暗号装置」、「楕円曲線に基づく公開鍵暗号装置」それぞれの基本は機能構成を述べ、後に、それぞれの各部における一実施例について説明する。まずは、「乗法群に基づく公開鍵暗号装置」について、

（１）鍵の生成

奇素数ｐ、ｑを任意に選び、$n = p^2 q$とする。ただし、ｐ、ｑのビット数は同じでｋとする。また、ＧＣＤ（ｐ，ｑ－１）＝１を満たしているとする。

【００２７】さらに、ｇを（Ｚ／ｎＺ）* の中から、$g_p = g^{p-1} \bmod p^2$ が（Ｚ／p^2 Ｚ）* の中での位数がｐとなるものを取る。すると、上述の関数ＬでＬ

（g_p）≠０mod ｐが成立する。実際、（Ｚ／p^2 Ｚ）* の中での位数がｐとなるものは１＋ｋｐmod p^2 （ｋはｐで割れない）と表せ、したがってＬ（１＋ｋｐ）＝（（１＋ｋｐ）－１）／ｐ＝ｋ≠０mod ｐとなるからである。また、具体的に、ｇを生成する方法としては、ランダムにｇを（Ｚ／ｎＺ）* から選ぶと、Ｌ（g_p）≠０mod ｐとなる確率は１－（１／ｐ）程度と考えられるので、無視出来ない確率で選ぶことが出来る。利用者は、公開は出来ないが、システムパラメータの一つとしてＬ（g_p）$^{-1}$mod ｐをあらかじめ計算しておくことに

（３）復号処理

暗号文Ｃの定義式（30）の両辺を、それぞれｐ－１乗すると、mod ｎでの合同式は、勿論、mod p^2 でも成立

$$C^{p-1} = g^{(p-1)(m+rn)} = g_p{}^m \times g_p{}^{rn} \bmod p^2 = g_p{}^m \bmod p^2 \quad (31)$$

従って

$$C_p = C^{p-1} \bmod p^2 \quad (32)$$

とおけば

$$C_p = g_p{}^m \bmod p^2 \quad (33)$$

C_p ，g_p ∈Γであるから、上述で定義した関数Ｌを使うと

$$L(C_p) = L(g_p{}^m) = mL(g_p) \bmod p \quad (34)$$

即ち

$$m = L(C_p) / L(g_p) \bmod p \quad (35)$$

となり、復号出来る。

【００３０】従って、復号処理を整理すると、まず、暗号文Ｃに対して、式（32）でC_p を計算し、次にＬ（C_p）を計算し、最後にＬ（C_p）と、あらかじめ計算しておくことが出来るＬ（g_p）$^{-1}$mod ｐとのmod ｐでの積を取って復号出来る。

（３）「乗法群に基づく公開鍵暗号装置」が、受動的攻撃に対して安全であることの証明。

【００３１】「乗法群に基づく公開鍵暗号装置」を解読することと、ｎを素因数分解することが同値であることを示す。ｎを無視できない確率で素因数分解するアルゴリズムが存在すれば、明らかに「乗法群に基づく公開鍵暗号装置」を解読する平均的多項式時間アルゴリズムが構成できるので、ここでは、次の事実のみを証明する：“「乗法群に基づく公開鍵暗号装置」を無視できない確率で解読するアルゴリズムＡ存在するならば、ｎを素因数分解する平均的多項式時間アルゴリズムを構成出来る”（ここで、上述の“ｎを無視できない確率で素因数分解するアルゴリズム”という意味は、そのアルゴリズムを入力ｎのビット数の多項式オーダー程度繰り返し適用することによって、かならず素因数分解出来るアルゴリズムのことである。以下、同様の使い方をする。厳密な定義は、文献１１を参照）

実際、今、合成数ｎ（＝p^2 ｑ）が与えられているとすると、ランダムにｇ∈（Ｚ／ｎＺ）* を選んで、この発明の公開鍵暗号装置のパラメータとして、無視できないする。

【００２８】従って、（ｎ，ｇ，ｋ）を公開鍵（ｐ，ｑ）を秘密鍵とする。ここでＬ（g_p）$^{-1}$mod ｐも秘密鍵と考えて良い。

（２）暗号化処理

平文ｍ（但し、０＜ｍ＜2^{k-1} ）に対して、まず、乱数ｒを０＜ｒ＜ｎの範囲から選び、ｍ＋ｒｎを計算し、暗号文Ｃは以下のように計算する。

【００２９】

$$C = g^{m+rn} \bmod n \quad (30)$$

し、g_p mod p^2 の位数はｐであり、ｒｎはｐの倍数であって$g_p{}^{rn}$＝１となるから、

確率でとることが出来て、次に、ｘをＺ／ｎＺからランダムに選ぶとき、ｘmod ｐＬＣＭ（ｐ－１，ｑ－１）の分布と、この発明の公開鍵暗号装置における、暗号化処理時の途中の計算に出てくる、ｍ＋ｒｎに対する、ｍ＋ｒｎ modｐＬＣＭ（ｐ－１，ｑ－１）の分布の差は、無視できる確率であることが証明できる。従って、Ｚ／ｎＺからランダムにｘを選び、Ｃ＝g^x mod ｎで計算されたＣは、無視できない確率で暗号文だと、アルゴリズムＡは認識し、Ｃに対応する平文x_0 を出力する。今、ｘが、ｘ＜2^{k-1} なる範囲の数となる確率は無視できるので、無視できない確率でｘ＞2^{k-1} としてよく、すると、ｘ≡x_0 （mod ｐ）、また、x_0 ＜2^{K-1} より、ｘ≡x_0 （mod ｎ）が不成立となり、したがって、ＧＣＤ（ｘ－x_0 ，ｎ）を計算すると、この値はｐ，ｐｑ，p^2 のいずれかとなり、ｎを素因数分解することが出来る。全体として、ｎのビット数の平均的多項式時間で素因数分解出来る。つまりｎを素因数分解することと同値であって、受動的攻撃に対する安全性が高い。

【００３２】次に、「楕円曲線に基づく公開鍵暗号装置」について、暗号の構成法、及び、変形素因数分解問題と等価であることについて述べる。まず最初に、復号に利用するＳＳＡアルゴリズムについて述べる。有限素体F_p 上の anomalous楕円曲線Ｅ上の離散対数問題とは、そのF_p －有理点Ｇ，Ｐが与えられたとき、Ｐ＝ｍＧとなるｍ∈Ｚ／ｐＺを求めることであるが、ＳＳＡアルゴリズムは、上でも述べたが、 anomalous楕円曲線上

の離散対数問題の解法を与えるアルゴリズムで、有限素体F_p上のanomalous楕円曲線であれば、ｐのビット数をｋとして、計算量はk^3のオーダーである効率的なアルゴリズムであって、具体的には次のような手順となる：

ＳＳＡアルゴリズム

入力：（Ｇ，Ｐ，Ｅ）

出力：ｍ

手順１　ＥをＺ上に持ち上げた楕円曲線Ｅ′で、Ｅ（F_p）からF_pへの写像λ_E'が、自明な写像にならないものを選ぶ。これは、ｐのビット数をｋとすれば、k^2のオーダーで計算できる。

手順２　手順１で構成した写像λ_E'を使ってλ_E'（Ｇ），λ_E'（Ｐ）を計算し（これはk^3のオーダーで出来る）、$m=\lambda_E'(P)/\lambda_E'(G) \bmod p$を計算する（これは、$k^3$のオーダーで出来る）

いずれにしても、ｐのビット数をｋとすれば、ＳＳＡアルゴリズムの計算量はk^3のオーダーである。このλ_E'は、Ｅ（F_p）からF_pへの群としての同型写像をあたえる。なお、λ_E'の構成方法など、詳しくは、文献１０を参照。またｐが５以下であればＳＳＡアルゴリズムを用いることなく効率的に解ける。

（１）鍵の生成

奇素数ｐ、ｑを任意に選び、ｎ＝ｐｑとする。ただし、ｐ、ｑのビット数は同じでｋとする。次に、F_p上のanomalous楕円曲線E_p，F_q上のanomalousでない楕円曲線E_qを選ぶ：

$$E_p : y^2 = x^3 + a_p x + b_p \quad (a_p, b_p \in F_p,\ 4a_p^3 + 27b_p^2 \neq 0), \tag{36}$$

$$E_q : y^2 = x^3 + a_q x + b_q \quad (a_q, b_q \in F_q,\ 4a_q^3 + 27b_q^2 \neq 0), \tag{37}$$

但し、$\#E_p(F_p)=p$，$\#E_q(F_q)=q'=q+1-t$（$-2\sqrt{q}<t\leq 2\sqrt{q}$，$t\neq 1$，$q'\neq p$）を満たすとする。#は集合の元（要素）の数を表わす。期待する位数を持つ楕円曲線の構成方法は、虚数乗法論を援用した比較的効率の良い生成方法が提案されていて、特に、anomalous楕円曲線の生成については、例えば、IEICE Trans.Fundamentals,E76-A,1,pp.50-54(1993)において、“Elliptic Curve Suitable for Cryptography”と題して、Miyaji，Ａ．により論及されている。（以下、この文献を文献１２と称す）さらに、$E_p(F_p)$，$E_q(F_q)$各々の点G_p，G_qで、位数が$\mathrm{ord}(G_p)=p$，$\mathrm{ord}(G_q)=q'$なるものを選ぶと仮定する。ここで、$E_q(F_q)$は、一般には巡回群になるとは限らないが、ここでは簡単のためこう仮定しておく。一般には、q'が十分大きな素因子をもつようなものにし、その大きな素数を位数とする点をG_qと取って良い。次に、中国人剰余定理を使って、Ｚ／ｎＺ上の楕円曲線E_nを作る：

$$E_n : y^2 = x^3 + ax + b \quad (a,b \in Z/nZ, \mathrm{GCD}(4a^3+27b^2, n)=1) \tag{38}$$

すなわち、すでに定義した記号で書けば

$$E_n = [E_p, E_q],\ a=[a_p, a_q],\ b=[b_p, b_q] \tag{39}$$

である。また

$$G=[G_p, G_q] \tag{40}$$

としておく。

【００３３】さらに、ＳＳＡアルゴリズムを用いて、公開はせずに、システムパラメータの一つとしてあらかじめ$\lambda_{Ep}'(G_p)^{-1} \bmod p$を計算しておく。これも秘密鍵の一つとして考えて良い。以下、簡単のために、この写像をλと書く。従って、（ｎ，E_n，Ｇ，ｋ）を公開鍵、（ｐ，ｑ）を秘密鍵とする。ここで、E_p，E_q，G_p，G_q，$\lambda(G_p)^{-1} \bmod p$も秘密鍵と考えてもよい。

（２）暗号化処理

平文ｍ（但し、$0<m<2^{k-1}$）に対して、まず、乱数ｒを$0<r<n$の範囲から選び、$m+rn$を計算し、暗号文Ｃは以下のように計算する。

【００３４】

$$C=(m+rn)G \in E_n(Z/nZ) \tag{41}$$

（３）復号処理

暗号文Ｃの定義式（４１）の両辺を、それぞれ$\bmod p$とすると、$rnG \bmod p=0$となるから、

$$C_p = (m+rn)G_p = mG_p \in E_p(F_p) \tag{42}$$

但し、これは、楕円曲線E_n上の加法を用いて、点Ｇを$m+rn$倍したものであって、暗号文が楕円曲線上の点であることに注意。すなわち、二つのＺ／ｎＺの元の組である。（あえて書けば、Ｃ＝（Ｃｘ，Ｃｙ），Ｃｘ，Ｃｙ∈Ｚ／ｎＺ）

なる、anomalous 楕円曲線における離散対数問題に変換される。ここで、$C=[C_p, C_q]$とおいた。

【００３５】従ってＳＳＡアルゴリズムを用いてｍは求められる。実際、λの準同型性により、

$$\lambda(C_p) = \lambda(mG_p) = m\lambda(G_p) \bmod p \tag{43}$$

即ち

$$m=\lambda(C_p)/\lambda(G_p) \bmod p \quad (44)$$

となり、復号出来る。

【００３６】従って、復号処理を整理すると、まず、暗号文Ｃに対して、$C=C_p \bmod p$を計算し、次に$\lambda(C_p)$を計算し、最後に$\lambda(C_p)$と、あらかじめ計算しておくことが出来る$\lambda(G_p)^{-1} \bmod p$との$\bmod p$での積を取って復号出来る。

（３）「楕円曲線に基づく公開鍵暗号装置」が、受動的攻撃に対して安全であることの証明。「楕円曲線に基づく公開鍵暗号装置」を解読することと、公開鍵（ｎ，E_n，Ｇ，ｋ）という情報からｎを素因数分解することが同値であることを示す。即ち、変形素因数分解問題と同値であることを示す。

【００３７】ｎを無視できない確率で素因数分解するアルゴリズムが存在すれば、明らかに「楕円曲線に基づく公開鍵暗号装置」を解読する平均的多項式時間アルゴリズムが構成できるので、ここでは、次の事実のみを証明する：“「楕円曲線に基づく公開鍵暗号装置」を無視できない確率で解読するアルゴリズムＢ存在するならば、ｎを素因数分解する平均的多項式時間アルゴリズムを構成出来る”（ここで、上述の“ｎを無視できない確率で素因数分解するアルゴリズム”という意味は、そのアルゴリズムを入力ｎのビット数の多項式オーダー程度繰り返し適用することによって、かならず素因数分解出来るアルゴリズムのことである。以下、同様の使い方をする。厳密な定義は、文献１１を参照）

実際、今、合成数ｎ（＝ｐｑ）が与えられているとすると、ｚをＺ／ｎＺからランダムに選ぶとき、ｚ$\bmod$ＬＣＭ（ｐ－１，ｑ－１）の分布と、我々の公開鍵暗号システムにおける、暗号化処理時の途中の計算に出てくる、ｍ＋ｒｎに対する、ｍ＋ｒｎ $\bmod pq'$ の分布の差は、無視できる確率であることが証明できる。従って、Ｚ／ｎＺからランダムにｚを選び、$C=zG \in E_n$（Ｚ／ｎＺ）で計算されたＣは、無視できない確率で暗号文だと、アルゴリズムＢは認識し、Ｃに対する平文z_0を出力する。今、ｚが、$z<2^{k-1}$なる範囲の数となる確率は無視できるので、無視できない確率で$z>2^{k-1}$としてよく、すると、$z \equiv z_0 \pmod p$、また、$z_0<2^{k-1}$より、$z \equiv z_0 \pmod n$が不成立となり、したがって、ＧＣＤ（$z-z_0$，ｎ）を計算すると、この値はｐとなり、ｎを素因数分解することが出来る。全体として、ｎのビット数の平均的多項式時間で素因数分解出来る。

【００３８】次に、この発明の「乗法群における公開鍵暗号装置」、「楕円曲線に基づく公開鍵暗号装置」それぞれの、実施例について説明する。まずは、「乗法群における公開鍵暗号装置」の一実施例について説明する。図１に示すように、暗号装置１００と復号装置２００が通信回線３００により接続されている。暗号化装置１００は、指数生成部１１０と法ｎでの巾乗計算器１２０を有す。復号装置２００は、Γ－変換器２１０と離散対数解法部２２０を有する。

【００３９】まず、暗号化装置１００での暗号化処理について説明する。暗号化装置１００における指数生成部１１０の詳細を図に示す。指数生成部１１０は、暗号化装置１００の利用者から平文（ｍ）を受けとると、乱数生成器１１１は乱数$r \in Z/nZ$を発生させ、これを乗算器１１２に入力して、ｒｎを計算し、これを加算器１１３に入力してｍ＋ｒｎを計算し、この結果をｎ－巾乗計算器１２０に入力して、暗号文$C=g^{m+rn} \bmod n$を生成する。

【００４０】次に、復号装置２００での復号処理について説明する。復号装置２００におけるΓ－変換器２１０の詳細を図２Ｂに示す。また、離散対数解法部２２０の詳細を図４に示す。復号装置２００におけるΓ－変換部２１０は、通信回線３００から、暗号文（Ｃ）を受けとると、$\bmod p^2$－還元器２１１で$C \bmod p^2$を計算し、この値をΓ－変換器２１２に入力して、$C_p=C^{p-1} \bmod p^2$を計算し、C_pを離散対数解法部２２０に入力する。離散対数解法部２２０は、Γ－変換部２１０からC_pを受けとると、それを、対数計算機２２１に入力し、$L(C_p)$を計算する。次に、これを、乗算器２２２に入力し$L(C_p) \times L(g_p)^{-1} \bmod p$を計算する。この値を、離散対数解法部２２０は復号平文ｍとして出力する。

【００４１】次は、「楕円曲線に基づく公開鍵暗号装置」の一実施例について説明する。図３にこの発明の一実施例を示す。暗号装置４００と復号装置５００が通信回線６００により接続されている。暗号化装置４００は、指数生成部４１０とE_n－巾乗計算器４２０を有す。復号装置５００は、$\bmod p$－還元器５１０とＳＳＡアルゴリズム部５２０を有する。

【００４２】まず、暗号化装置４００での暗号化処理について説明する。暗号化装置４００における指数生成部４１０の詳細を図４Ａに示す。指数生成部４１０は、暗号化装置４００の利用者から平文（ｍ）を受けとると、乱数生成器４１１は乱数$r \in Z/nZ$を発生させ、これを乗算器４１２に入力して、ｒｎを計算し、これら加算器４１３に入力してｍ＋ｒｎを計算し、この結果をE_n－巾乗計算器４２０に入力して、暗号文Ｃ＝（ｍ＋ｒｎ）Ｇを生成する。

【００４３】次に、復号装置５００での復号処理について説明する。復号装置５００におけるＳＳＡアルゴリズム部５２０の詳細を図４Ｂに示す。復号装置５００における$\bmod p$－還元器５１０は、通信回線６００から、暗号文（Ｃ）を受けとると、$C_p=C \bmod p \in E_p(F_p)$を計算し、$C_p$をＳＳＡアルゴリズム部５２０に入力する。ＳＳＡアルゴリズム部５２０は、$\bmod p$－還元器５１０からC_pを受けとると、それを、対数計

算機５２１に入力し、λ（C_p）を計算する。次に、これを、乗算器５２２に入力しλ（C_p）×λ（G_p）$^{-1}$ mod pを計算する。この値を、ＳＳＡアルゴリズム部５２０は復号平文mとして出力する。

【００４４】

【発明の効果】以上説明したように、この発明によれば、素因数分解問題の困難さを仮定した上で、ある種の安全性の証明のついた、今までにない新しい公開鍵暗号システムを構成することが出来る。従って、現在ではnが１０２４ビット程度であれば、nを素因数に分解することは現実的には困難であるから、nを１０２４ビット程度以上にしておけば十分安全なものとなる。

【００４５】暗号化処理、復号処理の計算量は共に、k^3 のオーダーであって、現在までに知られている代表的な公開鍵暗号と比べても同程度であり、非常に実用的な暗号であるとも言える。さらに、受動的攻撃に対する安全性が証明されているため、現在もっとも有力と考えられているＲＳＡ暗号よりも安全なことが保証される。

【図面の簡単な説明】

【図１】この発明の「乗法群に基づく公開鍵暗号装置」における暗号装置と復号装置の一実施例の機能構成を示すブロック図。

【図２】Ａは図１中の指数生成部１１０の具体的機能構成例を示すブロック図、Ｂは図１中のΓ－変換部２１０の具体的機能構成例を示すブロック図、Ｃは図１中の離散対数解法部２２０の具体的機能構成例を示すブロック図である。

【図３】この発明の「楕円曲線に基づく公開鍵暗号装置」における暗号装置及び復号装置の各実施例の機能構成を示すブロック図。

【図４】Ａは図３中の指数生成部４１０の具体的機能構成例を示すブロック図、Ｂは図３中のＳＳＡアルゴリズム部５２０の具体的機能構成例を示すブロック図である。

【図１】

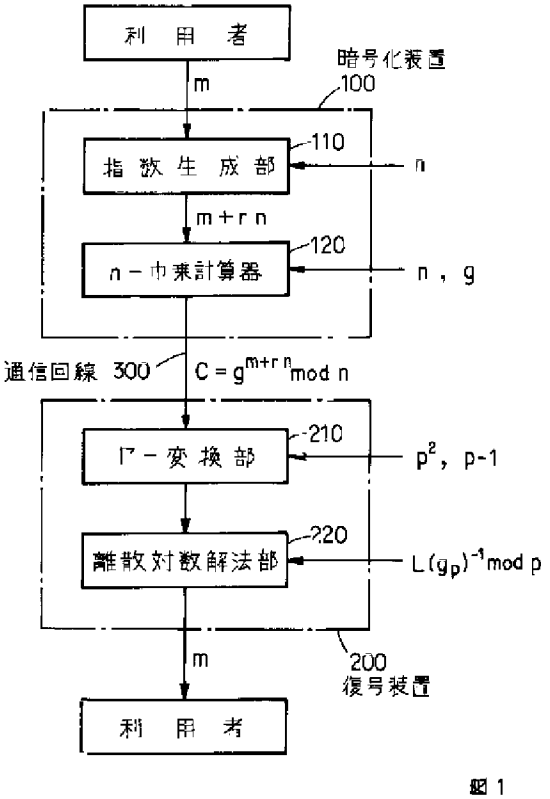


図 1

【図２】

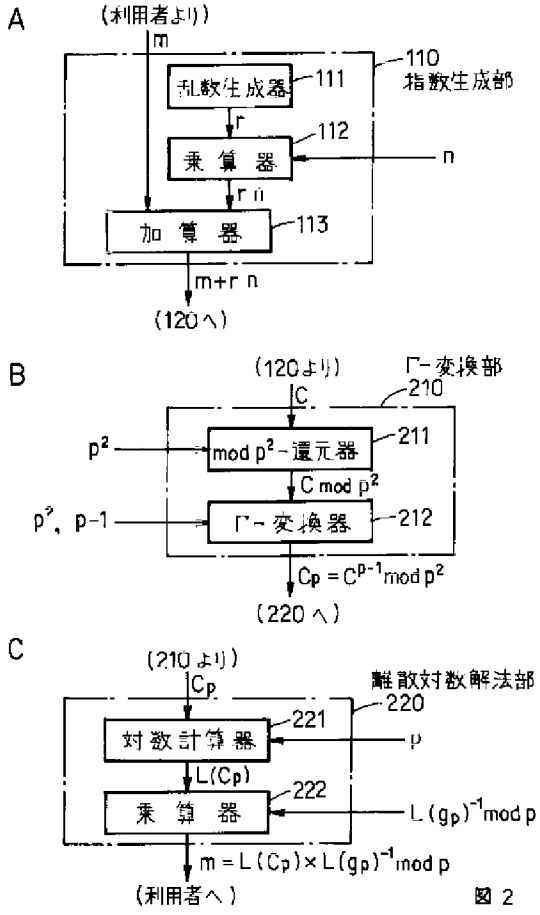


図 2

【図３】

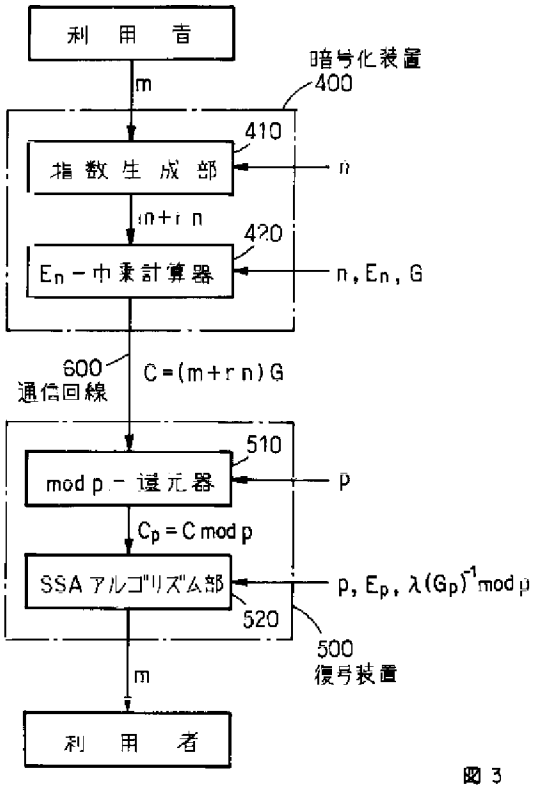


図３

【図４】

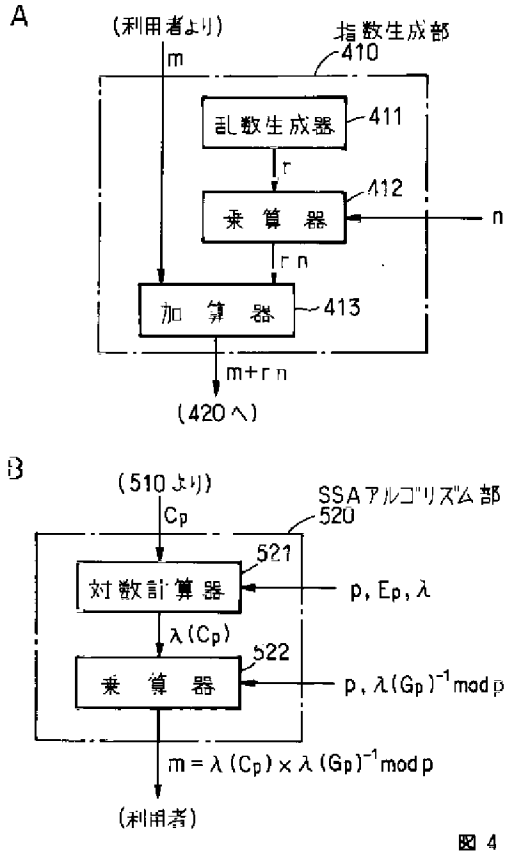


図４

【手続補正書】
【提出日】平成１１年２月１６日
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】請求項６
【補正方法】変更
【補正内容】
【請求項６】　公開鍵ｎ，ｇを用いる暗号化装置の暗号化処理を実行するプログラムを記録した記録媒体において、
上記プログラムは、
乱数ｒを生成する過程と、
上記乱数ｒと上記公開鍵ｎを乗算する過程と、
その乗算結果ｒｎと入力平文ｍを加算する過程と、
上記公開鍵ｎを法として、上記公開鍵ｇに対し上記加算値ｍ＋ｒｎを巾乗計算して暗号文Ｃを出力する過程とよりなることを特徴とするコンピュータ読出し可能な記録媒体。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】請求項１０
【補正方法】変更
【補正内容】
【請求項１０】　入力された平文と乱数を組み合わせて指数を生成する指数生成手段と、
合成数よりなる第１公開鍵を法として剰余類環上との楕円曲線における巾乗計算を、上記指数を指数とし、第２公開鍵に対して行って暗号文を出力する巾乗計算手段と、
を具備する公開鍵暗号化装置。
【手続補正３】
【補正対象書類名】明細書
【補正対象項目名】００２５
【補正方法】変更
【補正内容】
【００２５】この発明の「楕円曲線に基づく公開鍵暗号装置」においては、暗号化装置は、平文と乱数を組み合わせて、E_n（Ｚ／ｎＺ）における巾乗計算のための指数部分を生成する指数生成部、E_n（Ｚ／ｎＺ）での巾乗計算を行う、E_n-巾乗計算器からなり、E_n-巾乗計算器で生成された暗号文を通信回線に送出する。一方、復号装置は、E_n（Ｚ／ｎＺ）の点をE_p（F_p）の点に変換するmod ｐ－還元器と、E_p（F_p）における離散

対数問題を解いて復号する、ＳＳＡアルゴリズム部から　　なる。